Tissue V2 Features

- Definitions:
  - Detector: a process (piece of software) used to find issues. A Tissue detector defines the default parameters for all associated issues and a list of valid reporting nodes.
  - Issue: a security/configuration policy item.
    The complete security/configuration policy will have many items, some of which are defined as Tissue issues. A Tissue issue has parameters that determine if the resulting tissue event will request a network block.
  - Tissue System: a MISCOMP system/cluster or temporarily registered device (e.g. laptop).
  - Event: a Tissue System/Issue/Timestamp tuple.
    Events are tracked (i.e. they have a workflow) which causes emails to be sent, timeouts and network blocks to be scheduled.
  - Exemption: a Tissue System (MISCOMP registered or temporarily registered) with an exemption type of “whitelist”, “scan” or “issue”, expiration timestamp and behavior (“ignore”, “toss”, “email only”). In Phase II, an exemption behavior will include various nmap scan parameters).
  - Repeat Detection: a reported event for a Tissue System/issue that matches an existing open event.
  - Repeat Offense: a reported event for a Tissue System/issue that matches a “recently closed” event. The definition of “recently closed” is closed within the configured issue timeout.

- Features:
  - Consolidated exemptions for systems and issues:
    Tissue systems can be exempt from all/selected issues. In Phase II, Tissue systems can be exempt from various scan parameters (e.g. 64K ports, aggressive). Guest registered systems (single MAC address) can be exempt from all/selected issues. Exempting a Tisue system will exempt all MISCOMP registered interfaces (MAC addresses). Phase II will include the exemption workflow (request, approval, expiring reminder, etc.).
  - Exemptions for Virtual Machines:
    Exemptions for Virtual Machines will exempt the VM Host and hence all running VMs. This is a defect in the way MISCOMP records interfaces. The interfaces for individual VMs cannot be distinguished in MISCOMP.
  - All event remediations will be authenticated.
    If a user can't authenticate (via KCA or LDAP) to the Tissue GUI, the Service Desk will perform the remediation. This means that any pending remediations are the result of specifying “remediation approval required” in either the detector or issue parameters.
  - Events now correctly handle repeat detection and repeat offenders.
    Reports (GUI web pages) will show counts of repeated detections and offenders per event.
  - Remediation approval required will be available per issue.
    In Phase II, a remediation approval work flow will be available.
  - Repeat detection for open/pending events and repeat offense for closed (remediated) events will be recognized.
    A repeat offense within the issue timeout will reopen the old (closed) event, otherwise a new event is created. A reopened event will have all email, timeouts and blocks rescheduled just like a new event. As a result of this, the event log will now contain all relevant information...open, remediation, close, repeat, remediation, close etc. This should make identifying "problem" systems easier.
  - Detectors will contain one or more issues.
    Detectors will be easy to create and will encourage using more detectors with a few issues. This will simplify the current situation where one detector (VSCAN) contains the majority of issues. Detectors are configured with the same parameters as issues. Issues will inherit default parameters from their detector parent.
  - Emails will be formatted using a template system.
    The email template is specified in the detector and can be overridden in the issue. The template system will make available selected "internal" values such as all configured email addresses (to:, from:, cc:, reply-to:), configured keywords, timeout, block_delay,